

RELATÓRIO TÉCNICO DE INVESTIGAÇÃO DIGITAL

Análise OSINT, técnica e de risco do domínio

sssbra1.com

Objeto investigado	sssbra1.com - espelho “BRA” da casa de apostas e cassino online SSSGAME
Natureza	Verificação de legitimidade regulatória e de identidade do operador
Data da coleta	17/11/2026 (RDAP, DNS, HTTP/TLS, geolocalização, bases públicas, análise do código da página)
Métodos	OSINT passivo · RDAP · DNS · HTTP/TLS · análise do HTML e dos scripts
Achado central	Espelho da SSSGAME com o mesmo build de sssgame11.com, fora do `.bet.br`, ainda acessível no DNS de provedor brasileiro
Classificação	**RISCO ALTO**
Emissão do laudo	18/11/2026 as 00:54

1. Sumário Executivo

Este laudo documenta a investigação técnica do endereço **sssbra1.com**, realizada em **17/11/2026** por técnicas de OSINT (inteligência de fontes abertas) e análise passiva — requisições equivalentes às de um visitante comum e consultas a bases públicas, sem cadastro, sem compra e sem envio de dados pessoais. Toda evidência foi preservada em arquivo e teve seu hash SHA-256 calculado (Anexo A).

O endereço entrega a aplicação “sssgame - Apostas Desportivas Online”, cuja descrição promete “a casa de apostas online mais popular do mundo” e mistura português e inglês (“Get your exclusive welcome offer when you join Sssgame today”). O domínio integra a rede de marca **SSSGAME**: o hub sssgame777.com lista dezesseis espelhos numerados (sssgame2, sssgame11, sssgame22 … sssgame999) com código de indicação, e sssbra1.com e sssgame11.com servem exatamente o mesmo build de aplicação.

O primeiro problema é regulatório. Desde a regulamentação das apostas de quota fixa no Brasil, o operador autorizado pelo Ministério da Fazenda opera obrigatoriamente sob domínio `.bet.br`. A consulta ao Registro.br mostra que **sssgame.bet.br** não existe (RDAP 404), e o domínio investigado é um gTLD genérico. Diferentemente de sssgame11.com e sssgame777.com, este espelho **ainda resolve** no DNS do provedor brasileiro usado na coleta — o que é coerente com a estratégia de rotação de domínios.

CLASSIFICAÇÃO DE RISCO **RISCO ALTO**

Leitura: o nome “sssbra1” sugere um espelho voltado ao Brasil criado para substituir domínios já bloqueados; o apostador não tem operador identificado a quem recorrer (Seções 4 e 5).

2. Metodologia e Cadeia de Custódia

Empregaram-se exclusivamente **técnicas passivas**. As respostas de rede e de bases públicas foram salvas no momento da coleta e tiveram hash SHA-256 calculado. O DNS foi consultado via resolvedor público 1.1.1.1; o conteúdo, os cabeçalhos e o bundle JavaScript foram obtidos por requisição HTTPS de visitante comum. Nenhum formulário foi preenchido e nenhum dado pessoal foi enviado. Fuso de referência: UTC.

Etapa	Técnica / fonte	Evidência preservada
Registro do domínio	RDAP (rdap.org / registro do gTLD / Registro.br)	`rdap_raw.json · rdap_*.json`
DNS	dig (A, AAAA, NS, MX, TXT, SOA, CNAME) via 1.1.1.1	`dns_records.txt`
Conteúdo / cabeçalhos	curl HTTPS (visitante comum) e navegador headless; home, páginas legais e scripts	`corpo_*.html · headers_home.txt · bundle*.txt`
Certificado TLS	openssl s_client / x509	`tls_cert.txt`
Geolocalização do IP	ipinfo.io · PTR reverso	`geoip.json`
CNPJ declarado	Validação por módulo 11 · base pública BrasilAPI/Receita	`cnpj_publico_*.json`
Consolidação	Extração de fatos e hashes SHA-256	`hash_manifest.txt`

3. Identificação Técnica (Domínio, DNS, Hospedagem e TLS)

Domínio	sssbra1.com
Registro	27/11/2024 · expira 27/11/2028 · **720 dias** antes da coleta
Titular	**Oculto** no RDAP (o registro expõe apenas o registrador)

Registrador	Name.com, Inc. · abuse@name.com
Servidores de nome	finley.ns.cloudflare.com · sandra.ns.cloudflare.com
DNS - A	104.21.40.182 · 172.67.137.87 · sem MX
Hospedagem	AS13335 Cloudflare, Inc. · San Francisco/US · cabeçalho `server: cloudflare`
Certificado TLS	Google Trust Services (WE1) · emitido em 06/11/2026 · válido até 04/02/2027
Domínio .bet.br	**sssgame.bet.br não registrado** (Registro.br, RDAP 404)
Build	Mesmos arquivos `/client/assets/*` (hashes idênticos) de sssgame11.com

Leitura: domínio de 2024 (Name.com) com titular oculto e renovação até 2028, NS e proxy Cloudflare, certificado Google Trust Services emitido em 06/11/2026.

4. Plataforma, Fluxo de Pagamento e Dados Coletados

Aplicação de página única idêntica à de sssgame11.com; o conteúdo é carregado por script após o login.

Aspecto	Constatação
Produto	Apostas esportivas e cassino online
Rede	Build idêntico a sssgame11.com (listado no hub sssgame777.com)
Operador	Não identificado; sem licença, sem CNPJ
Texto	Descrição em português e inglês, “a casa de apostas mais popular do mundo”

Leitura: depósitos e saques ocorrem dentro da aplicação, fora de qualquer supervisão brasileira.

5. Indicadores de Risco

#	Indicador	Evidência	Sev.
1	Apostas fora do .bet.br; sssgame.bet.br inexistente	`rdap_raw.json`	ALTA
2	Mesmo build de espelho já sem resolução no DNS brasileiro	`corpo_home.html`	ALTA
3	Operador não identificado	`corpo_home.html`	ALTA

Síntese: três indicadores, todos de severidade alta.

6. Conclusão Técnica e Recomendações

O sssbra1.com é um espelho ativo da casa de apostas SSSGAME, com o mesmo build de um domínio já sem resolução no DNS de provedor brasileiro. Classificação técnica: **RISCO ALTO** — oferta de apostas ao público brasileiro fora do regime autorizado, por operador não identificado.

Recomendações ao consumidor / solicitante

- No Brasil, só operam legalmente as casas de apostas autorizadas pelo Ministério da Fazenda, sob domínio `.bet.br`; consulte a lista oficial da SPA/MF antes de depositar.
- Não instale aplicativos (APK) baixados fora das lojas oficiais nem informe CPF e dados bancários a operadores sem identificação verificável.
- Em disputa com operador fora do regime autorizado, o apostador não conta com a proteção da regulamentação brasileira para reaver saldo ou saques.

Recomendações de mitigação / denúncia

- Reportar o endereço ao Google Safe Browsing e ao canal de abuso do registrador (abuse@name.com).
- Comunicar à Secretaria de Prêmios e Apostas (SPA/MF) e à Anatel a oferta de apostas ao público brasileiro fora do regime autorizado.
- Vítimas que pagaram via Pix: acionar o banco imediatamente pedindo o MED (Mecanismo Especial de Devolução), registrar boletim de ocorrência e reclamação em consumidor.gov.br / Procon, anexando este laudo.

Ressalva: este laudo expressa **juízo técnico de risco** com base em evidências públicas coletadas passivamente em 17/11/2026; não é decisão judicial e não imputa crime a nenhuma pessoa física ou jurídica. Registradores, provedores de hospedagem/CDN, plataformas de loja e intermediários de pagamento são citados apenas como fatos técnicos, sem imputação de conduta. O titular do site pode usar estes achados para corrigir as inconsistências apontadas. Os fatos podem mudar após a coleta.

Anexo A - Manifesto de Integridade (SHA-256)

Hashes SHA-256 das evidências preservadas no momento da coleta (cadeia de custódia).

Arquivo	SHA-256
corpo_home.html (234584 bytes)	352561855eba92a32abe7ba724e87c2c3cd5c06bb90f5bcc6a02b8e76ea1c0fd
dns_records.txt (362 bytes)	bed8a65fead592972e39736de059006432aba3da98c0626fed5c5b1a668a2d19
geoip.json (288 bytes)	b86d9c71695859d79c3a390c573c088603d8e9663a85571a2b714cd9b4b28f7b
headers_home.txt (1365 bytes)	cafb0bf49b304d533477e66d2a7d0b619e152b4b686f6b259074ba562d02fb9f
rdap_raw.json (2547 bytes)	986bc88b5b0ae0b5609e82a6391eed6779b3800a5a8217e4ec91da1233cab078
tls_cert.txt (300 bytes)	1f7d9138e754d71a3a95fbbbc0850326e9dbd0504840f7bdbba8aa90bbd44344

- Fim do relatório -